05-PR-M-0002

Issuance date: **28 February 2006**
Update: 22 September 2006
Update: 9 March 2007

INFORMATION ASSURANCE (IA) TRAINING AND CERTIFICATION:
VERSION 2.0

1. Overview:

The IA workforce focuses on the operation and management of IA capabilities for Department of Defense (DoD) systems and networks. IA ensures that adequate security measures and established IA policies and procedures are applied to all Information Systems (IS) and networks. The IA workforce includes all privileged users and IA managers who perform any of the responsibilities or functions described in DoD 8570.01-M Chapters 3 – 5. These responsibilities include: developing, testing, deploying, operating, administering, troubleshooting, managing, and retiring Department of Defense (DoD) information systems. To support the warfighter in a highly effective and professional manner, the Army must ensure that appropriate levels of IA awareness, training, education, certification, and workforce management are provided to the IA workforce and IS users that commensurate with their respective responsibilities.

The IA training audience includes military, civilian, foreign nationals and contractor personnel in Deployed and Generating Forces organizations. In addition to being able to demonstrate the required level of technical and/or managerial skills and experience, it is DoD policy (DoDD 8570.1) that "the IA workforce knowledge and skills be verified through standard certification testing." Consequently, Army IA personnel must attain and maintain Information Technology (IT)/IA certifications appropriate for the technical and/or managerial requirements of their position. In some cases, this will include passing one or more certification exams. IA Workforce personnel in Technical and Management Level positions must complete eighty hours of sustainment training biannually or as required to maintain certification status, whichever is greater.

This Best Business Practice (BBP) describes regulatory requirements established by the DoD 8570.01-M the process for requesting a certification voucher (appendix 1). The IA workforce, technical, and management levels described in DoD 8570.01-M are listed in this BBP. Programs such as, network compliance scanning and vulnerability assessments will also have training addressed in their respective BBPs.

References:

AR 25-2 – Information Assurance, dated 14 November 2003.

DoD Directive 8570.1 (DoDD 8570.1) Information Assurance Training, Certification, and Workforce Management, 15 August 2004.

DoD 8570.01-M – Information Assurance Workforce Improvement Program, dated 19 December 2005.

Memorandum: Manpower and Reserve Affairs, Payment of Expenses to Obtain Professional Credentials for Army Civilian Employees, dated 20 June 2003.

2. Point(s) of Contact (POC):
NETCOM ESTA / OIA&C

Phyllis Bailey	Phyllis.bailey@us.army.mil	(703) 602-7408; DSN 332
Doris Wright (CONT SPT)	doris.wright@us.army.mil	(703) 602-7420; DSN 332
Group email address	iawip@us.army.mil	

3. Description of Former State: Army and DoD regulations did not require specific certification and training at different levels. This BBP provides the training and certification requirements for Technical and Management levels.

4. Description of Changes Instituted: The IA Workforce must become familiar with the training and certification requirements in accordance with their title and position. Personnel who have privileged access and limited privileged access (IT-1 and IT-II) are required to be IA trained, certified and maintain their certifications. All managers need to be fully aware that foreign nationals can not be IT-1 without consent of the Local Designated Approving Authority (DAA), the data owner and approval by HQDA CIO/G6.

5. Description of End State: An IA trained and certified workforce with enhanced capabilities to combat threats against Army information, networks, and IS.

6. Description of Required Resources: Army is working with DoD to decrease the cost for obtaining a commercial certification. Military personnel can use the GI Bill to cut the cost for the COMPTIA Security+, A+, Network+, among others. They must contact their education center for more information. Civilians and Military are authorized to pay for certification training through their appropriate organization's funds per memorandum (see References, below) and H.R 1815 National Defense Authorization Act for Fiscal Year 2006 – Payment for Professional Credentials. E-learning provides training that builds on some commercial certification courses; certification testing cannot be taken online. The cost of individual certification tests range from $100 to $500. There are additional costs for TDY, tuition, and travel costs for specific technical training.

7. Description of Derived Benefits Resulting from Implementation: A more secure use of Army information, networks, and IS in support of the warfighter and garrison activities, including the reduction of vulnerabilities that can be exploited due to systems and networks being administered by an inadequately trained and unskilled workforce.

8. Administrative Requirements:

a. The minimum IA training requirements must be completed within six months of assignment to IA duties. Certification and validated testing (with a passing score), must be completed in accordance with the individual's performance and evaluation process. This includes duties as system/network administrators, IA positions, i.e., Information Assurance Manager (IAM), Information Assurance Security Officer (IASO), Information Assurance Network Managers (IANM), and Information Assurance Program Manager (IAPM) staff. Refresher training is required between 18 to 24 months, after initial training (AR 25-2a (8) (a)).)). All individuals in Technical positions must sign a Privileged-Level Access Agreement (PAA). The PAA will be completed and kept on file along with their appointment orders. Management level certifications are cumulative (you must have a certification at each Management level even if you are in Management Level III), Technical level certifications are not cumulative (if you are certified at a higher level, you do not also have to hold a certification at the lower level.

b. The E-Learning modules (SkillPort) for IA training are available at https://usarmy.SkillPort.com via the AKO portal at https://www.us.army.mil. Contractors who require access to SkillPort for IA training will send their request through their IAM or IAPM with the NETCOM IA Division Point of Contacts (POC) at iawip@us.army.mil.

c. The IA workforce will provide initial information and status updates as they complete training/certification courses in the Asset and Vulnerability Tracking Resource (A&VTR) Database. New IA workforce personnel will register in A&VTR at time of appointment. DoD policy requires status of all positions with IA responsibilities, regardless of occupational specialty, or whether the duty is performed full-time or part-time as an additional/embedded duty. Each of these positions will be aligned to an IA category, level, and documented in the appropriate database.

d. IA workforce personnel are encouraged to pursue educational opportunities through the IA Scholarship Program (IASP) to obtain advanced degrees with IA concentrations.

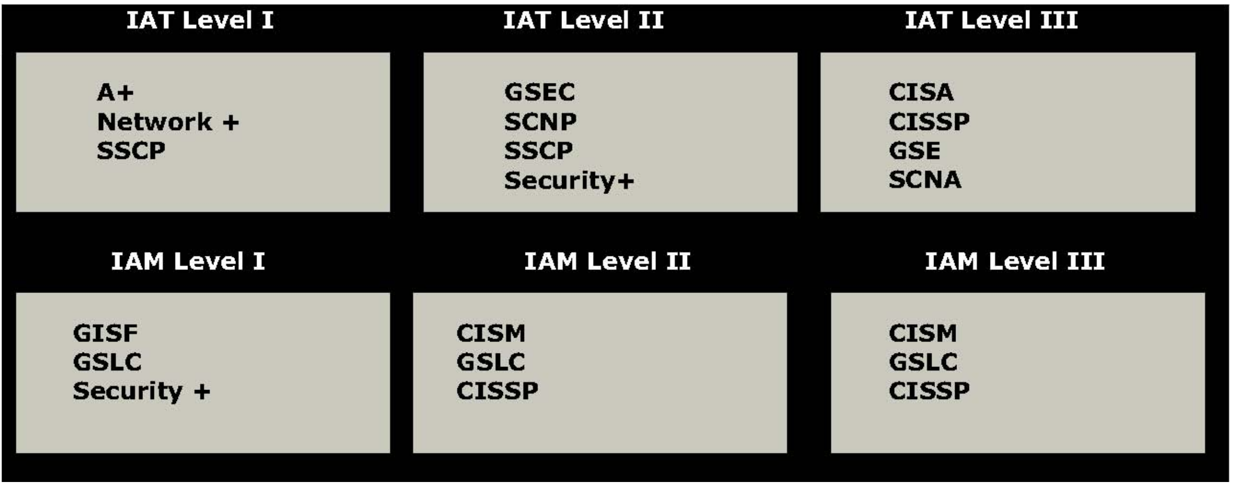
9. Related BBPs:

06-PR-M-0003 Privileged –Level Access Agreement (PAA) Acceptable Use Policy (AUP) BBP
04-EC-O-0004 Network Assessment Scanning

10. Products:

- E-learning (SkillPort) is available at https://usarmy.skillport.com
- DISA web-based training available at http://www.iase.disa.mil
- MACOM-approved IT/IA training and vendor specific training uniquely focused on passing certification tests.
- IASP program is: http://www.defenselink.mil/nii/iasp/.
- Manpower and Reserve Affairs Memorandum, Subject: Payment of Expenses to Obtain Professional Credentials for Army Civilian Employees: http:/cpol.army.mil/library/train/tld-062003.html.
- Virtual training: https://iatraining.us.army.mil
- Credentialing Opportunities On-line (COOL) site: https://www.cool.army.mil/
- Appendix 1 to IA training and Certification BBP: Army Voucher Process and Procedures

Table1: DoD Approved Baseline Certifications



IAT Level I	IAT Level II	IAT Level III
A+ Network + SSCP	GSEC SCNP SSCP Security+	CISA CISSP GSE SCNA
IAM Level I	**IAM Level II**	**IAM Level III**
GISF GSLC Security +	CISM GSLC CISSP	CISM GSLC CISSP

11. Description: Refer to Table 1, IA Workforce Certification (abstract from DoD 8570.01-M) for IAT and IAM training certifications**.** Personnel in technical level positions are also required to obtain computing environment certifications. Examples of computing environment certifications are MCSE, MCDBA, CCNP, CWNP and CCNA. The training and certification requirements for the IA roles and the IA workforce are listed under the titles, as follows:

Management Levels: All must obtain a Commercial Certification

a. **Management Level I: Information Assurance Security Officer (IASO) and Information Management Officers (IMO)/Information Systems Officers (ISO):** Complete the minimum training requirements within 6 months of assuming the position. Complete all minimum training requirements prior to enrollment in a schoolhouse course. Personnel who fill the position should have 0-5 years of management experience and be knowledgeable in their organization's Computing Environment. The IASO/IMO/ISO will be designated as Information Technology I (IT-I/II/or III).

Minimum Training Requirements:

(1). IASO course online (https://ia.gordon.army.mil/iaso) – estimated time: 2-3 working days.

(2). E-learning Security + modules (SkillPort, CIO G6/NETCOM IA Phase I>SYO-101 Security+ (5 modules)) – estimated time: 3-4 working days.

(3). IA Technical Level 1 course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) – estimated: 5-7 working days.

Certification Requirements:

The IASO/IMO/ISO will complete one of the certifications listed in Table 1. The type of baseline certification will be determined by the IA professional's supervisor during the performance evaluation process.

b. **Management Level II: Installation/Major Subordinate Commands (MSC)/posts, Army Commands (AC)/Army Service Component Command (ASCC))/ Direct Reporting Units (DRU)/Tactical Units/PEOs/ all other tenant activities (if connected behind Army firewalls) Level Information Assurance Manager (IAM), and Agent of the Certification Authority (ACA):** Complete the minimum training requirements within six (6) months of assuming the position. Personnel who fill the position should have at least five (5) years of management experience and must be knowledgeable in their organization's Network Environment. Management Level II personnel must be knowledgeable of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure Network Environment. They typically report to an IA Management Level III (Enclave) Manager, DAA, or senior management for network operational requirements. The IAM position is designated as IT-I/II or III per AR 25-2. The CA is designated as IT-I per AR 25-2.

Minimum Training Requirements:

(1). IASO course online (https://ia.gordon.army.mil/iaso) – estimated time: 2-3 working days.

(2). E-learning - Certified Information Systems Security Professional (CISSP) modules (SkillPort, CIO G6/NETCOM IA Phase I> Certified Information Systems Security Professional (CISSP) – 5 modules) – estimated time: 3-5 working days

(3). CD ROM, DoD Certifier Fundamentals from http://iase.disa.mil **(ACA only complete item 3 all others complete items 1 and 2)** estimated: 1.5 hour. ACA must also complete items 1 and 2 if dual-hatted in a management position with valid appointment orders.

Certification Requirements:

The Level II manager will complete one of the Management Level II certifications listed in Table 1. The completion of certification testing is required. The type of certification will be determined by the IA professional's supervisor during the performance evaluation process. Management Level II personnel will obtain the appropriate Management Level I certification.

c. **Management Level III: Regional Chief Information Office Director and Information Assurance Program Manager (IAPM)//Certification Authority (CA) (AC/ASCC/DRU and RCIO level)**: Complete the minimum training requirements within six (6) months of assuming the position. Personnel who fill the position should have at least ten (10) years of management experience and must be knowledgeable in their Regional Enclave Environment. They must be knowledgeable of IA policy, procedures, and workforce structure to develop, implement and maintain a secure enclave environment. Management Level III Director/IAPM/CA typically reports to a DAA for IA issues and senior managers for enclave operational requirements. These individuals need to be able to translate strategic plans and technical guidance provided by NETCOM into objectives, strategies, and architectural guidance.

Minimum Training Requirements:

(1). IASO course online (https://ia.gordon.army.mil/iaso) – estimated time: 2-3 working days.

(2). E-learning - Certified Information Systems Security Professional (CISSP) modules (SkillPort, CIO G6/NETCOM IA Phase I> Certified Information Systems Security Professional (CISSP) – 5 modules) – estimated time: 3-5 working days. .

(3). CD ROM, DoD Certifier Fundamentals from http://iase.disa.mil **CA only complete item 3 all others complete items 1 and 2)** estimated: 1.5 hour. CA must also complete items 1 and 2 if dual-hatted in a management position with valid appointment orders or the 4012 certificate.

Certification Requirements:

The Level III manager will complete one of the Management Level III certifications listed in Table 1. The completion of certification testing is required. The type of certification training will be determined by the IA professional's supervisor during the performance evaluation process. Management Level III personnel will also obtain the appropriate Management Level I and II certifications.

d. **Management Level III: DAA**: Complete the minimum training upon DAA appointment by CIO/G6. The DAA must be a U.S. citizen and have a level of authority commensurate with accepting, in writing, the risk of operating IS under his/her purview.

(1). Complete the Army specific DAA training module. DAAs can access this module through the Army's Virtual Website at https://iatraining.us.army.mil. This module is part of the DIACAP implementation process.

(2). Complete the DoD DAA computer-based training (CBT) product for certification. The CBT title, "DAA Designated Approving Authority," is available at http://iase.disa.mil/ . The completion certificate will be signed by the DAA and the IAPM. The certificate of completion will be maintained as part of the DAA's official personnel file.

(3). The DAA must recertify every three (3) years.

(4). If the DAA is performing other management functions, i.e., IAM-II or IAM-III, they must meet the minimum training and certifications requirements for those categories and levels.

e. **Management Level** personnel who hold a **valid baseline certification** and have a minimum of one (1) year in their position at their organization:

(1). Complete the IASO online course – estimated time: 2-3 working days.

(2). Maintain the certification IAW the standards of the certifying body.

Technical Levels: All must obtain a Baseline Commercial and Computing Environment Certification

f. **Technical Level I:** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO). Complete the minimum training requirements within six (6) months of assuming the position. Normally the Level I SA/NA/IANM/IANO has 0-4 years of experience in IA technology or a related field and must be knowledgeable in their organization's Computing Environment (CE). They must know how to apply basic knowledge of IA concepts, practices and procedures within the CE. Level I SA/NA/IANM/IANOs are usually individuals with limited privileged access to the Computing Environment and works under immediate supervision and typically reports to a Computing Environment manager. They are designated as IT-II per AR 25-2. **Technical Level I certification is required prior to being authorized unsupervised privileged access**

Minimum Training Requirements:

(1). IASO course (https://ia.gordon.army.mil) – estimated time: 2-3 working days

(2). IA Technical Level I course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification – 11 modules) – estimated time: 5-7 working days.

(3). Network Security Issues (SkillPort>CIO-G6/NETCOM Information Assurance>CIO - G6/NETCOM IA Phase I>Net Safety>Network Security Issues – 1 module (estimated time: 3.5 hours).

(4). Completion of an on-the-job skills practical evaluation to meet functional requirements of DoD 8570.01-M. This requirement must be validated by the individual IAPM or IAM.

Certification Requirements:

The Level I technical person will complete one of the Technical Level I certifications listed in Table 1. The completion of certification testing is required. The type of certification training will be determined by the IA professional's supervisor during the performance evaluation process. Technical Level I personnel will also obtain the appropriate computing environment certification/s.

g. **Technical Level II:** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO). Complete the minimum training requirements within six (6) months of assuming the Technical Level II SA/NA/IANM/IANO position. Normally the Level II SA/NA/IANM/IANO has 3-7 years of experience in IA technology or a related field and must be knowledgeable in their organization's NE and advance training in their CE. Complete all minimum training requirements prior to enrollment in a schoolhouse course. Level II technicians must master the functional requirements of the IA Technical Level I position and be able to apply knowledge and experience with standard IA concepts, practices and procedures within the network environment. The Level II SA/NA/IANM/IANO is usually an individual with **Privileged Access** to the Computing Environment and works under general supervision and typically reports to a Level III NM. They are designated as IT-I per AR 25-2.

Minimum Training Requirements:

(1). IASO course (https://ia.gordon.army.mil) – estimated time: 2-3 working days

(2). IA Technical Level I course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) – estimated time: 5-7 working days.

(3). E-learning Security + modules (SkillPort, CIO G6/NETCOM IA Phase I>SYO-101 Security+ (5 modules)) – estimated time 3-4 working days.

(4). Level II, one week Security+ training course formerly known as the SA/NM course. Schedule and locations located at http://ia.gordon.army.mil. –Must register through the Army Training Requirements and Resources Systems (ATRRS).

(5). Completion of an on-the-job skills practical evaluation to meet functional requirements of DoD 8570.01-M. This requirement must be validated by the individual IAPM or IAM.

Certification Requirements:

The Level II technical person will complete one of the Technical Level II certifications listed in Table 1. The completion of certification testing is required. The type of certification training will be determined by the IA professional's supervisor during the performance evaluation process. Technical Level II personnel will also obtain the appropriate computing environment certification/s. The Technical Level II supervisor will notify the IA professional if she/he needs to attend the Technical Level III certification courses held at the National Guard Bureau (NGB) Professional Education Center (PEC) or Fort Gordon, School of Information Technology training facilities.

h. **Technical Level III:** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO). Complete the minimum training within six (6) months of assuming the position. Normally the Technical Level III SA/NA/IANM/IANO has seven (7) years of experience in IA technology or a related field and must be knowledgeable in their organization's Network Engineer (NE) and advance training in their Computer Engineer (CE). They must be subject matter experts (SMEs) in all functional requirements of IA Technical Level I and IA Technical Level II positions. Complete all minimum training requirements prior to enrollment in a schoolhouse course. They must be able to apply extensive knowledge of a variety of IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems. They work independently to quickly and completely solve problems and may lead and direct the work of others. Typically they report to an Enclave Manager. They are designated as IT-I per AR 25-2.

Minimum Training Requirements

(1). IASO course (https://ia.gordon.army.mil) – estimated time: 2-3 working days.

(2). IA Technical Level I course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) – estimated time: 5-7 working days.

(3). E-learning Security + modules (SkillPort, CIO G6/NETCOM IA Phase I>SYO-101 Security+ (5 modules)) – estimated time 3-4 working days.

(4). Level II, one week Security+ training course formerly known as the SA/NM course. Schedule and locations located at http://ia.gordon.army.mil. –Must register through the Army Training Requirements and Resources Systems (ATRRS).

(5). Completion of an on-the-job skills practical evaluation to meet functional requirements of DoD 8570.01-M. This requirement must be validated by the individual IAPM or IAM.

Certification Requirements:

The Level III technical person will complete one of the Technical Level III certifications listed in Table 1. The completion of certification testing is required. The type of certification training will be determined by the IA professional's supervisor during the performance evaluation process. Technical Level III personnel will also obtain the appropriate computing environment certification/s. The Technical Level III supervisor will notify the IA professional if she/he needs to attend the Technical Level III certification courses held at the National Guard Bureau (NGB) Professional Education Center (PEC) or Fort Gordon, School of Information Technology training facilities.

i. **Technical Level II and III – holding valid certifications:** System Administrator (SA)/ Network Administrator (NA)/Information Assurance Network Manager (IANM)/Information Assurance Network Officer (IANO).. SA/NA/IANM/IANO with a valid certification in the IATII or IATIII levels, a valid Computing Environment Certification and at least one (1) year in the position at their assigned organization must complete the following:

Training Requirements:

(1). IASO course (https://ia.gordon.army.mil) – estimated time: 2-3 working days.

(2). IA Technical Level I course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification – 11 modules) – estimated time: 5-7 working days.

(3). Complete an on-the-job skills practical evaluation to meet functional requirements of DoD 8570.01-M. This requirement must be validated by the individual IAPM or IAM.

Certification Requirements:

Technical Level II and III personnel will continue their sustainment training/continuing education as required to maintain certification.

12. Awareness Training: Orientation and annual IA awareness training for users are mandatory. The trained and aware employee is the first and most vital line of defense in protecting Information and IS. This training must be documented by the IASO or IAM.

Minimum requirements:

(1). E-learning- US Army Information Assurance Awareness module, https://usarmy.skillport.com.

(2). Users without SkillPort accounts can go to the Fort Gordon website at www.ia.gordon.army.mil to take the User Awareness training – estimated time: 1 hour

(3). MACOM/RCIO/CIO G-6 approved IA awareness training course, with electronic record of student attendance.

13. Refresher training: Training for IA positions (IAPM, IANM, IAM, IASO, IMO, ISO, SA/NA, IANM/IANO, DAA, and CA) is required every 18-24 months. The methods listed below will satisfy the refresher training requirement.

a. Army IA Workshop.

b. E-learning – IA Custom Path Phase II> IDO 470 Security Professional (5 modules) – estimated time: 2-3 working days (estimated average total time: 24 hours and 45 minutes).

c. E-learning – IA Custom Path Phase 1> GIAC security fundamentals (15 modules) – estimated time: 3-5 working days.

d. E-learning - IA Technical Level I course (11 modules) – estimated time: 5-7 working days. (Do not take as a refresher if it is already annotated in the minimum training requirements).

e. Other service or DoD IA workshops (capture date in A&VTR).

14. Recertification: Complete the applicable vendor or vendor-neutral recertification as required to maintain certification.

15. Equivalencies: The following courses are equivalent to the minimum training requirements for Managers: CNSS 4011 certificate course or the National Defense University, Information Resources Management College (IRMC) Advanced Management Program completion. DAAs may substitute the CNSS 4012 certificate for the CBT or IRM college Advanced Management Program completion. Course attendance does not constitute certification. Passing a certification exam is mandatory to meet DoD 8570.01-M requirements.

16. IA Tools: Users of STAT, Retina, Hercules, and Retina Enterprise Management (REM) will complete the training at https://informationassurance.us.army.mil. Users attending the Computer Defense Assistance Program (CDAP) training, formerly called the Do-It Yourself Vulnerability Assessment Program (DITYVAP) are trained on the Retina Scanner.

17. Tactical Unit IA Awareness training/reporting capability: The IA Workforce should train their users in garrison to minimize bandwidth issues when units are deployed. The tracking of completions will be done through the Army Training Requirements and Resource System (ATRRS) link with SkillPort.

18. Timelines: Organizations must meet the following milestones. The milestones will begin in organizations' next planning, IA program and budget cycle in Fiscal Year 2007 (FY07).

a. Year one: 31 December 2006- Identify IA workforce positions fill 10 percent of the IA positions with trained certified personnel and develop a budget to support follow on implementation for years two – four

b. Year two: (FY 07) **-** Fill a total of 40 percent of the IA positions with trained and certified personnel

c. Year three: (FY 08) - Fill a total of 70 percent of the IA positions with trained and certified personnel

d. Year four: (FY-09) **-** All valid IA positions are held by trained and certified personnel. Thereafter, all incumbents and new hires must be trained, certified, and recertified in their current position.

19. Definitions:

a. Privileged access: Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access: (a) "Super user," "root," or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth; (b) Access to change control parameters (for example, routing tables, path priorities, addresses) of router, multiplexers, and other key information system or network equipment or software; (c) Ability and authority to control and change program files, and other users' access to data; (d) Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed; or (e) Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operation.

b. Limited privileged access: Privilege access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

c. Computing Environment : Workstation or server host and its operating system, peripherals, and applications.

d. Network Environment (Computer): The constituent element of an enclave responsible for connecting CE by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

e. On the job training (OJT): Supervised hands on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

f. Enclave: Collection of CE connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in OMB A-130 (reference (i)). Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers

Table 2: IA Workforce Certification Organizations

Certification Provider	Certification Name
Computing Technology Industry Association (CompTIA)	A+
CompTIA	Security +
CompTIA	Network+
International Information Systems Security Certifications Consortium (ISC)2	Certified Information Systems Security Professional (CISSP)
(ISC)2	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Manager (CISM)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Auditor (CISA)
SecurityCertified.Net	Security Certified Network Professional (SCNP)
SecurityCertified.Net	Security Certified Network Architect (SCNA)
SANS Institute	GIAC Security Essentials Certification (GSEC)
SANS Institute	GIAC Security Leadership Certificate (GSLC)
SANS Institute	GIAC Security Expert (GSE)
SANS Institute	GIAC Information Security Fundamentals (GISF)

Table 3: Training and Certification Matrix

Personnel with no certification	IA Mgmt 1	IA Mgmt 2	IA Mgmt 3	IA Tech 1	IA Tech 2	IA Tech 3	DAA	CA
Training Requirement 1	IASO online course	IASO online course	IASO online course	IASO online course	IASO online course	IASO online course	Army Specific DAA training module	DoD Certifier fundamentals
Training Requirement 2	Security + (SkillPort)	CISSP (SkillPort)	CISSP (SkillPort)	IA Technical Level I (SkillPort)	IA Technical Level I (SkillPort)	IA Technical Level I (SkillPort)		IASO online course – if working in a management position
Training Requirement 3				Network Security Issues (SkillPort)	Technical Level II SA/NM course	Technical Level II SA/NM course		CISSP (SkillPort)- if working in a management position
Training Requirement 4				On the job skills practical evaluation	On the job skills practical evaluation	On the job skills practical evaluation		
Authorized Substitutes		CNSS 4011 certificate	CNSS 4011 certificate				CNSS 4012 certificate	
Certification Requirement	Obtain the appropriate certification for this level.	Obtain the appropriate certification for this level.	Obtain the appropriate certification for this level.	Obtain the appropriate certification for this level-for privilege access.	Obtain the appropriate certification for this level.	Obtain the appropriate certification for this level.	DoD DAA CBT	
Privileged-Level Access Agreement Required				Yes w/valid certification	Yes	Yes		
***Certified* personnel: Baseline & CE for Technical level; Baseline only for Mgmt, Both must have at least 1 year on job experience)**	IA Mgmt Level I	IA Mgmt Level II	IA Mgmt Level III	IA Tech Level I	IA Tech Level II	IA Tech Level III		
Training Requirement 1	IASO online course	IASO online course	IASO online course	IASO online course	IASO online course	IASO online course		
Training Requirement 2				IA Technical Level I (SkillPort)	IA Technical Level I (SkillPort)	IA Technical Level I (SkillPort)		
Training Requirement 3				On the job skills practical evaluation	On the job skills practical evaluation	On the job skills practical evaluation		
Certification Requirement	Maintain the certification you hold IAW the standards of the certifying body.	Maintain the certification you hold IAW the standards of the certifying body.	Maintain the certification you hold IAW the standards of the certifying body.	Maintain the certification you hold IAW the standards of the certifying body.	Maintain the certification you hold IAW the standards of the certifying body.	Maintain the certification you hold IAW the standards of the certifying body.		
Privileged-Level Access Agreement				Yes w/valid certification	Yes	Yes		

Army Voucher Process and Procedures
Appendix 1

Objective: Military and Government Civilians to include, Non Appropriate Funds (NAF) and Foreign Nationals performing IA functions described in DoD 8570.01-M "Information Assurance Workforce Improvement Program" are eligible to receive a voucher through Army and/or their respective organization. Individuals must be trained in their IA duties and approved by their Information Assurance Manager and/or supervisor. Contractors and State employees can not receive vouchers through this process.

Requirements:

1. Have at least 1 year left in the position and/or moving to another IA position within 6 months.

2. Be nominated by their IAM/ supervisor.

3. Complete minimum training requirements specified for their IA position IAW paragraph 11 of this document.

4. Have appointment orders and/or a signed Privileged-Level Access Agreement (PAA). See Privileged – Level Access Agreement (PAA) Acceptable Use Policy (AUP) BBP for an example.

5. Working in a Technical or Management IA position.

6. Network Operation and Security Center IA professionals must have their positions verified in the pilot Army's training and certification tracking database by their leadership and a signed PAA.

Vouchers:

Army will purchase a limited number of IA commercial certification vouchers to achieve some of the certifications outlined in DoD 8570.1-M baseline certification chart. All vouchers will be managed and distributed by OIA&C. Individuals receiving initial vouchers should test within 3 months of voucher request, or it will be reissued to another user. Individuals who do not pass on the first try will be given 3 months to complete additional studies in order to pass a second examination. The individual's IAM/supervisor is responsible for retraining and then requesting another voucher for a specific commercial certifications.

Certification examination: Exams are offered in a variety of ways, times and locations. Check with your local base or station education office for the schedule and location of certification exams in your area. You should verify certification exam date and location before you request a voucher. Certification certificates will be mailed to you directly from the certification exam provider upon successfully completing your exam. Once you have your certification certificate ensure your personnel records and the Pilot Training and Certification Tracking System are updated to reflect this significant accomplishment and requirement. Individuals are not required to pay.

Retraining alternatives: Training is provided to the IA workforce by distributed and/or as a blended solution. E-learning provides training in Security+, CISSP, A+, Network+, and GSEC. The Fort Gordon School of Information Technology provides training in Security+, CISSP, SSCP (Fort Gordon, Warrant Officer Course only). All of the surrounding mirror sites provide training on Security+. Training is free to Military, Government civilians, and contractors however organizations must pay individuals' TDY cost. Army recommends that organizations use the free resources to retrain their IA workforce.

Tracking System Registration Process: Individuals requesting a certification voucher will:

1. Go to https://iastar.net/army to register on the **Pilot** Army Training and Certification Tracking System.

2. Go to Registration Information and click on Register on this Web Site (Click Here).

3. Fill in all the fields then click "Register." Make sure you annotate your AKO email address.

4. The system will send a password to your AKO email address.

5. Once you receive your password, log back on the system and answer the job function questionnaire.

6. Your Technical I-III or Management I-III profile will be created.

7. Input your training completions and commercial certifications obtained. List the cert Id so it can be validated.

8. Input your Awareness training date (annual or initial).

9. Go to the main page and take the pre-assessment test for the CompTIA certification test.

10. Provide a copy of the pre-assessment test to your IAM/supervisor. A score of at least 75% is required to receive a voucher.

11. The supervisor/manager will verify the individual's profile level.

12. Input date/training for On the Job Training (OJT) that has been conducted under "OJT."

13. Once the individual is ready for an examination voucher, send an email to iawip@us.army.mil. The individual's training and profile level will be rechecked by the Office of Information Assurance and Compliance.

14. If the individual meets all the requirements the voucher will be added to their profile and sent to their email address. The individual then needs register for an exam at the appropriate testing center.

Pre-assessments procedures: DoD has acquired pre-assessment tests from Computing Technology Industry Associations (CompTIA) and SANS Technology Institute. The password and userid to access the CompTIA pre-assessment were provided in separate emails for each RCIO IAPMs. All Program Executive Offices (PEO) can send an email to iawip@us.army.mil for logon credentials. This information will be used to log on the website to take the pre-assessment test prior to obtaining a certification voucher from the Office of Information Assurance and Compliance. Individuals will take the appropriate pre-assessment prior to obtaining a certification exam voucher. A score of at least 75% is required to receive a voucher.

1. CompTIA pre-assessments procedures

a. Go to http://currency.comptia.org/dod from a computer that is connected the internet and a printer.

b. Enter: Name, Organization name and your .mil email address.

c. Enter: Organization's **User ID and password** provided by your RCIO IAPM or call/email iawip@us.army.mil

d. Select preferred assessment:
PC Technician = A+ objectives
Network Technologies = Network+ objectives
IT Security = Security+

e. Complete assessment

f. Print results and send to IAM/supervisor

2. SANS Institute - pre-assessments procedures

a. You need a SANS Portal Account (If you have not already created a SANS Portal account, create one at https://portal.sans.org.).

b. Go to SANS OnDemand web page at (www.sans.org/OnDemand/).

c. Users must be on a DoD ".mil" account to access the test site. Click on the yellow "Register" button under the heading "Assessment Only."

d. Complete the application page by following all three (3) steps listed (contact information, Track/Certification pre-assessment you want to take (must be the SANS GIAC Security Essentials Certification GSEC, Security Leadership Certificate GSLC, or Information Security Fundamentals GISF),

e. The discount code is (**DoD8570**), and click "Proceed."

f. Answer the questions on the next page and select "Check" as a payment option.

g. You will receive an "Order is Complete" message on the next page and a follow-up confirmation Email. You can also download your invoice or view your invoice at https://portal.sans.org/history (it will be for $0, no payment due).

h. when your assessment is uploaded into your SANS Portal Account, you will receive a 2nd confirmation email. Under your Welcome message in your Portal account, click on the SANS OnDemand link and start your assessment.